

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-162506

(43)Date of publication of application : 06.06.2003

(51)Int.Cl. G06F 15/00  
G06F 1/00  
G06T 1/00  
H04N 7/173

(21)Application number : 2001-358041

(71)Applicant : SONY CORP

(22)Date of filing : 22.11.2001

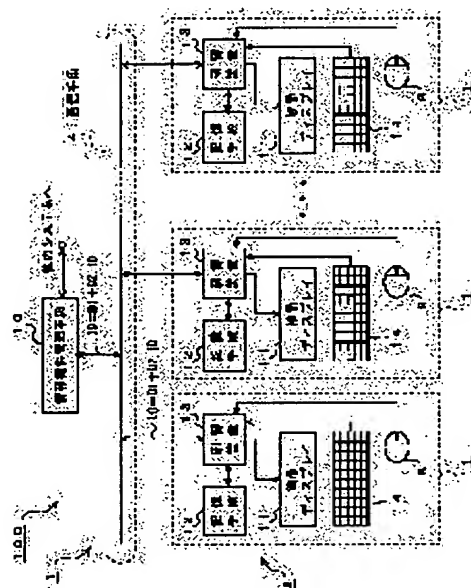
(72)Inventor : ISOZAKI MASAOKI

(54) NETWORK INFORMATION PROCESSING SYSTEM, INFORMATION- PROVIDING MANAGEMENT APPARATUS, INFORMATION-PROCESSING APPARATUS AND INFORMATION-PROCESSING METHOD

(57)Abstract:

実施形態としてのネットワーク情報処理システム100の構成例

PROBLEM TO BE SOLVED: To reject participation by unauthorized users to a system and preventing electronic equipment for a network configuration including an information providing management group from unauthorized use by a third party.  
SOLUTION: A network information processing system 100 comprising more than one information processing apparatus 1, having a GUI (graphical user interface) function to process any information, an information providing management means 10 processing information transmitted from the processing apparatuses 1 to provide electronic information contents and a communication means 4 connecting the management means 10 to each processing apparatus 1, where authentication processing to authenticate personal identification, by using the GUI function of the processing apparatuses 1. For example, if personal information read out from face image information D1 does not match the personal information presented from the third party, the system 100 can reject the participation in the system 100.



## LEGAL STATUS

[Date of request for examination]

14.03.2003

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

BEST AVAILABLE COPY

Copyright (C); 1998,2003 Japan Patent Office

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2003-162506

(P2003-162506A)

(43)公開日 平成15年6月6日(2003.6.6)

(51)IntCl. <sup>7</sup>	識別記号	F I	テマコード*(参考)
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 B 5 B 0 5 7
1/00	3 7 0	1/00	3 7 0 E 5 B 0 8 5
G 0 6 T 1/00	5 0 0	G 0 6 T 1/00	5 0 0 B 5 C 0 6 4
H 0 4 N 7/173	6 4 0	H 0 4 N 7/173	6 4 0 Z

審査請求 有 請求項の数35 O L (全 22 頁)

(21)出願番号 特願2001-358041(P2001-358041)

(22)出願日 平成13年11月22日(2001.11.22)

(71)出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72)発明者 五十崎 正明

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(74)代理人 100090376

弁理士 山口 邦夫 (外1名)

最終頁に続く

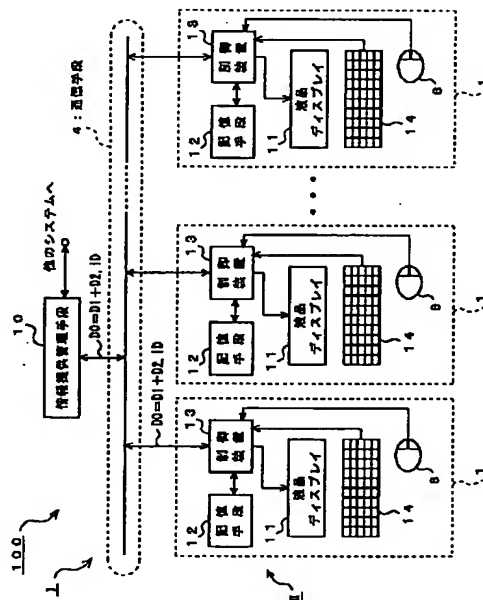
(54)【発明の名称】 ネットワーク情報処理システム、情報提供管理装置、情報処理装置及び情報処理方法

(57)【要約】

【課題】 不正使用者の当該システムへの参加を拒否できるようにすると共に、当該情報提供管理系を含むネットワーク構成用の電子機器の第三者による不正使用を防止できるようにする。

【解決手段】 G U I 機能を有して任意の情報を処理する一以上の情報処理装置1と、少なくとも、情報処理装置1から転送される情報を処理し表示情報を含む電子情報内容を提供する情報提供管理手段10と、この情報提供管理手段10と各々の情報処理装置1とを接続する通信手段4とを備え、情報提供管理手段10又は情報処理装置1において、当該情報処理装置1のG U I 機能を利用して使用者本人を特定するための認証処理をするようにしたものである。例えば、顔画像情報D1から読み出した個人情報と、第三者から提示された個人情報とが一致しない場合は当該システム100への参加を拒否することができる。

実施形態としてのネットワーク情報処理システム100の構成例



## 【特許請求の範囲】

【請求項1】 複数のネットワーク構成用の電子機器が同一のネットワーク上に接続される情報処理システムであって、

入力操作機能を有して任意の情報を処理する一以上の情報処理装置と、

少なくとも、前記情報処理装置から転送される情報を処理し表示情報を含む電子情報内容を提供する情報提供管理手段と、

前記情報提供管理手段と各々の前記情報処理装置とを接続する通信手段とを備え、

前記情報提供管理手段又は情報処理装置において、当該情報処理装置の入力操作機能を利用して使用者本人を特定するための認証処理をするようにしたことを特徴とするネットワーク情報処理システム。

【請求項2】 前記情報提供管理手段において使用者本人を認証処理する場合であって、

予め前記情報処理装置から前記情報提供管理手段へ使用者の顔画像情報及び個人情報を登録請求し、

前記情報提供管理手段では、

前記情報処理装置によって登録された使用者の顔画像情報に個人情報を付加して管理すると共に、前記使用者の情報処理装置に対して登録済みを示すキー情報を配信し、

以後、前記情報提供管理手段に対して前記入力操作機能を利用して前記キー情報及び個人情報が提示されたとき、

前記情報提供管理手段では、

前記キー情報に基づいて前記顔画像情報から個人情報を読み出し、

読み出された前記個人情報と提示された個人情報とを比較照合して前記本人を認証するようにしたことを特徴とする請求項1に記載のネットワーク情報処理システム。

【請求項3】 前記情報処理装置において使用者本人を認証処理する場合であって、

予め前記情報処理装置から前記情報提供管理手段へ使用者の顔画像情報及び個人情報を登録請求し、

前記情報提供管理手段では、

前記情報処理装置によって登録された使用者の顔画像情報に個人情報を付加した使用者顔画像情報を作成すると共に、前記使用者の情報処理装置に対して前記使用者顔画像情報及び登録済みを示すキー情報を配信し、

以後、前記情報処理装置に対して当該入力操作機能を利用して前記キー情報が入力されたとき、

前記情報処理装置では、

前記キー情報に基づいて前記使用者顔画像情報から個人情報を読み出し、

読み出された前記個人情報と提示された個人情報とを比較照合して前記本人を認証するようにしたことを特徴とする請求項1に記載のネットワーク情報処理システム。

【請求項4】 前記使用者の顔画像内に本人を特定する個人情報を重ねし、

前記顔画像内に重ねられた個人情報を読み出して当該使用者本人を認証することを特徴とする請求項1に記載のネットワーク情報処理システム。

【請求項5】 前記情報提供管理手段を含むネットワーク構成用の電子機器を操作できる範囲を示した操作権情報が前記個人情報に付加されることを特徴とする請求項1に記載のネットワーク情報処理システム。

10 【請求項6】 前記個人情報は、

前記キー情報によって復号可能な情報に暗号化され、前記暗号化後の個人情報を前記使用者の顔画像内の上下の所定ラインを表示する画像表示情報に重ねられることを特徴とする請求項1に記載のネットワーク情報処理システム。

【請求項7】 前記使用者顔画像情報を構成する画像表示情報にはチェック情報が含まれ、

前記使用者の認証時に、

20 前記チェック情報に基づいて前記画像表示情報の符号ビットを加算し、

前記符号ビットを加算した加算結果と前記チェック情報による期待加算結果とを比較照合することを特徴とする請求項3に記載のネットワーク情報処理システム。

【請求項8】 前記比較照合の結果で、前記符号ビットを加算した加算結果と前記チェック情報による加算結果とが一致しない場合は、

当該システムへの前記使用者の参加を拒否し、又は、前記情報提供管理手段を含むネットワーク構成用の電子機器の使用権利を制限することを特徴とする請求項7に記載のネットワーク情報処理システム。

30 【請求項9】 前記使用者顔画像情報は、

特定の管理者によって作成され、前記情報提供管理手段へ登録し及び使用者の情報処理装置に発行するようになされることを特徴とする請求項3に記載のネットワーク情報処理システム。

【請求項10】 前記情報処理装置を不特定多数の使用により共通に操作する場合は、

40 予め前記情報提供管理手段へ登録しておいた自分の使用者顔画像情報を当該情報処理装置にダウンロードして使用することを特徴とする請求項3に記載のネットワーク情報処理システム。

【請求項11】 前記情報処理装置に表示手段が設けられ、

前記使用者の顔画像に付加された個人情報を前記入力操作機能を利用して表示することを特徴とする請求項1に記載のネットワーク情報処理システム。

【請求項12】 前記使用者が未認証である場合は、前記表示手段には当該使用者が未認証である旨の表示がなされることを特徴とする請求項1に記載のネットワーク情報処理システム。

【請求項 13】 少なくとも、使用者の情報処理装置から転送される情報を処理し表示情報を含む電子情報内容を提供する装置であって、  
前記情報処理装置から登録された使用者の顔画像情報及び個人情報記憶する記憶手段と、  
前記情報処理装置によって登録請求された使用者の顔画像情報に個人情報を付加して管理すると共に、前記使用者の情報処理装置に対して登録済みを示すキー情報を配信する制御装置とを備え、  
当該制御装置に対して前記情報処理装置から前記キー情報が提示されたとき、  
前記キー情報に基づいて前記顔画像情報から個人情報を読み出し、  
読み出された前記個人情報と提示された個人情報とを比較照合して前記本人を認証するようにしたことを特徴とする情報提供管理装置。

【請求項 14】 少なくとも、使用者の情報処理装置から転送される情報を処理し表示情報を含む電子情報内容を提供する装置であって、  
前記情報処理装置から登録請求された使用者の顔画像情報及び個人情報を記憶する記憶手段と、  
前記情報処理装置によって登録請求された使用者の顔画像情報に個人情報を付加した使用者顔画像情報を作成すると共に、前記使用者顔画像情報及び登録済みを示すキー情報を前記使用者の情報処理装置に配信する制御装置とを備えることを特徴とする情報提供管理装置。

【請求項 15】 前記使用者の顔画像内に本人を特定する個人情報を重畳し、  
前記顔画像内に重畳された個人情報を読み出して当該使用者本人を認証することを特徴とする請求項 14 に記載の情報提供管理装置。

【請求項 16】 前記個人情報は、  
前記キー情報によって復号可能な情報に暗号化され、  
前記暗号化後の個人情報を前記使用者の顔画像内の上下の所定ラインを表示する画像表示情報に重畳されることを特徴とする請求項 14 に記載の情報提供管理装置。

【請求項 17】 前記使用者顔画像情報を構成する画像表示情報にはチェック情報が含まれ、前記使用者の認証時に、  
前記チェック情報に基づいて前記画像表示情報の符号ビットを加算し、  
前記符号ビットを加算した加算結果と前記チェック情報による期待加算結果とを比較照合することを特徴とする請求項 14 に記載の情報提供管理装置。

【請求項 18】 前記比較照合の結果で、前記符号ビットを加算した加算結果と前記チェック情報による加算結果とが一致しない場合は、  
当該システムへの前記使用者の参加を拒否し、又は、前記情報提供管理手段を含むネットワーク構成用の電子機器の使用権利を制限することを特徴とする請求項 17 に

記載の情報提供管理装置。

【請求項 19】 前記使用者顔画像情報は、  
特定の管理者によって作成され、前記情報提供管理手段へ登録し及び使用者の情報処理装置に発行するようになされることを特徴とする請求項 14 に記載の情報提供管理装置。

【請求項 20】 使用者本人を認証するためのキー情報に基づいて任意の情報を処理する装置であって、  
前記キー情報を入力する入力手段と、  
予め取得された使用者顔画像情報及び登録済みを示すキー情報を記憶する記憶手段と、  
前記入力手段により入力されたキー情報に基づいて前記記憶手段から使用者顔画像情報を読み出すと共に前記使用者顔画像情報から個人情報を読み出し、前記使用者顔画像情報から読み出された前記個人情報と前記入力手段により入力された個人情報とを比較照合して前記使用者本人を認証する制御装置とを備えることを特徴とする情報処理装置。

【請求項 21】 前記使用者の顔画像を表示する表示手段が備えられ、  
前記使用者の顔画像に付加された個人情報を前記入力操作機能を利用して表示することを特徴とする請求項 20 に記載の情報処理装置。

【請求項 22】 前記使用者が未認証である場合は、  
前記表示手段には当該使用者が未認証である旨の表示がなされることを特徴とする請求項 20 に記載の情報処理装置。

【請求項 23】 入力操作機能を有して任意の情報を処理する一以上の情報処理系と、少なくとも、前記情報処理系から転送される情報を処理し表示情報を含む電子情報内容を提供する情報提供管理系とを準備し、  
前記情報提供管理系又は情報処理系において、当該情報処理系の入力操作機能を利用して使用者本人を特定するための認証処理をするようにしたことを特徴とする情報処理方法。

【請求項 24】 前記情報処理系と前記情報提供管理系とを通信手段により接続することを特徴とする請求項 23 に記載の情報処理方法。

【請求項 25】 前記情報提供管理系において使用者本人の認証処理をする場合であって、  
前記情報処理系から前記情報提供管理系へ使用者の顔画像及び個人情報を登録請求し、  
前記情報提供管理系では、  
前記情報処理系によって登録請求された使用者の顔画像に個人情報を付加して管理すると共に、前記使用者に対して登録済みを示すキー情報を配信し、  
以後、前記情報提供管理系に対して前記キー情報が提示されたとき、  
前記情報提供管理系では、  
前記キー情報に基づいて前記顔画像から個人情報を読み

出し、  
読み出された前記個人情報と提示された個人情報とを比較照合して前記本人を認証するようにしたことを特徴とする請求項 2 3 に記載の情報処理方法。

【請求項 2 6】 前記情報処理系において使用者本人の認証処理をする場合であって、  
前記情報処理系から前記情報提供管理系へ使用者の顔画像及び個人情報を登録請求し、  
前記情報管理提供系では、  
前記情報処理系によって登録請求された使用者の顔画像に個人情報を付加して使用者顔画像情報を作成すると共に、前記使用者に対して使用者顔画像情報及び登録済みを示すキー情報を配信し、  
以後、前記情報処理系に対して前記キー情報が提示されたとき、  
前記情報処理系では、  
前記キー情報に基づいて前記使用者顔画像情報から個人情報を読み出し、  
読み出された前記個人情報と提示された個人情報とを比較照合して前記本人を認証するようにしたことを特徴とする請求項 2 3 に記載の情報処理方法。

【請求項 2 7】 前記使用者の顔画像内に本人を特定する個人情報を重畳し、  
前記顔画像内に重畳された個人情報を読み出して当該使用者本人を認証することを特徴とする請求項 2 3 に記載の情報処理方法。

【請求項 2 8】 前記情報提供管理系を含むネットワーク構成用の電子機器を操作できる範囲を示した操作権情報を前記個人情報に付加することを特徴とする請求項 2 3 に記載の情報処理方法。

【請求項 2 9】 前記個人情報は、  
前記キー情報によって復号可能な情報に暗号化し、  
前記暗号化後の個人情報を前記使用者の顔画像内の上下の所定ラインを表示する画像表示情報に重畳することを特徴とする請求項 2 3 に記載の情報処理方法。

【請求項 3 0】 前記使用者顔画像情報を構成する画像表示情報にチェック情報を付加し、  
前記使用者の認証時には、  
前記チェック情報に基づいて前記画像表示情報の符号ビットを加算し、  
前記符号ビットを加算した加算結果と前記チェック情報による期待加算結果とを比較照合することを特徴とする請求項 2 6 に記載の情報処理方法。

【請求項 3 1】 前記比較照合の結果で、前記符号ビットを加算した加算結果と前記チェック情報による加算結果とが一致しない場合は、  
当該システムへの前記使用者の参加を拒否し、又は、前記情報提供管理手段を含むネットワーク構成用の電子機器の使用権利を制限することを特徴とする請求項 3 0 に記載の情報処理方法。

【請求項 3 2】 前記使用者顔画像情報を特定の管理者によって作成し、

前記情報提供管理系へ該使用者顔画像情報を登録すると共に、前記使用者顔画像情報を使用者の情報処理系に発行するようにしたことを特徴とする請求項 2 6 に記載の情報処理方法。

【請求項 3 3】 前記情報処理系を不特定多数の使用者により共通に操作する場合は、

予め前記情報提供管理系へ登録しておいた自分の使用者顔画像情報を当該情報処理系にダウンロードして使用することを特徴とする請求項 2 3 に記載の情報処理方法。

【請求項 3 4】 前記情報処理系に表示手段を設け、  
前記使用者の顔画像に付加された個人情報を前記情報処理系の入力操作機能を利用して表示することを特徴とする請求項 2 3 に記載の情報処理方法。

【請求項 3 5】 前記使用者が未認証である場合は、  
前記表示手段には当該使用者が未認証である旨の表示をすることを特徴とする請求項 3 4 に記載の情報処理方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ネットワーク会議システムや、ネットワーク教育システム、ネットワークゲームシステム等に適用して好適なネットワーク情報処理システム、情報提供管理装置、情報処理装置及び情報処理方法に関する。

【0002】詳しくは、任意の情報を処理する一以上の情報処理装置と、表示情報を含む電子情報内容を提供する情報提供管理手段とを通信手段により接続し、情報提供管理手段又は情報処理装置において、当該情報処理装置の入力操作機能を利用して使用者本人を特定するための認証処理をし、不正使用者の当該システムへの参加を拒否できるようにすると共に、当該情報提供管理手段を含むネットワーク構成用の電子機器の第三者による不正使用を防止できるようにしたものである。

【0003】

【従来の技術】近年、パーソナルコンピュータ（以下でパソコンという）を用いて作成したプレゼンテーション資料を会議室に持ち込んで、プレゼンタ（資料発表者）がそれを複数の会議参加者に対して電子機器を用いて発表する、いわゆる電子会議システムが採られる場合が多くなってきた。

【0004】この電子会議システムでは表示機器と資料発表者のノートパソコンとが接続される。この表示機器にはデータプロジェクタが使用され、パソコンで作成したプレゼンテーション資料が表示される。データプロジェクタ（以下で単にプロジェクタという）には、一人のプレゼンタ自身のノートパソコンが RGB ケーブルを通じて接続され、そのノートパソコンに表示されている画面を白壁等に投影するようになされる。白壁等に表示さ

れているプレゼンテーション資料は発表者が操作するマウスカーソルによって指し示すようになされる。つまり、白壁等には説明者が所有している資料のみが表示される。

【0005】最近では、ネットワーク対応のデータプロジェクトが登場している。このプロジェクトにはパソコン機能が内蔵されているものである。これによれば、説明者が自身のノートパソコン（以下で情報処理装置ともいう）からプレゼンテーションファイルをネットワーク経由でプロジェクトに転送し、そのプロジェクトのパソコン機能によりその内容を表示し投影するようになされる。

【0006】

【発明が解決しようとする課題】ところで、従来例に係る電子会議システムによれば、以下のような問題がある。

① ネットワーク構成用の電子機器の第三者による不正使用を防止しようとしたとき、当該電子会議システムにおいて、クライアント側の情報処理装置の画面上に参加者の顔写真等のユーザアイコンを表示し、当該システムへの参加可否を判別する方法が考えられる。

【0007】この場合、ユーザアイコンの作成及び登録を参加者側に自由に委ねてしまうと、第三者が不正に他人のユーザアイコンを使用して、当該電子会議に参加してしまうおそれがある。特に、参加者が支社から本社へ出向していたり、別の会議場所に居る場合などは、お互いの顔を確認し合うことができない場合が多い。このような場合に第三者が本人になりすまして会議に参加し、貴重なプレゼンテーション情報を盗用してしまうことが予想される。

【0008】② 当該電子会議システムにおいて、ユーザアイコンをクリックして相手を指定し、チャットやファイル転送等を行うような操作を導入しようとした場合に、なりすまし参加者相手に、誤ってチャットやファイルを転送してしまうおそれがある。従って、貴重なプレゼンテーション情報が漏洩してしまう危険性が高くなり、セキュリティ上で大きな問題となる。特に、不特定多数のユーザが共通のノートパソコンを情報処理装置として使用する場合には、ユーザアイコンの管理が益々重要になってくる。

【0009】そこで、この発明はこのような従来の課題を解決したものであって、不正使用者の当該システムへの参加を拒否できるようにすると共に、当該情報提供管理系を含むネットワーク構成用の電子機器の第三者による不正使用を防止できるようにしたネットワーク情報処理システム、情報提供管理装置、情報処理装置及び情報処理方法を提供することを目的とする。

【0010】

【課題を解決するための手段】上述した課題は、複数のネットワーク構成用の電子機器が同一のネットワーク上

に接続される情報処理システムであって、入力操作機能を有して任意の情報を処理する一以上の情報処理装置と、少なくとも、情報処理装置から転送される情報を処理し表示情報を含む電子情報内容を提供する情報提供管理手段と、この情報提供管理手段と各々の情報処理装置とを接続する通信手段とを備え、情報提供管理手段又は情報処理装置において、当該情報処理装置の入力操作機能を利用して使用者本人を特定するための認証処理をするようにしたことを特徴とするネットワーク情報処理システムによって解決される。

【0011】本発明に係るネットワーク情報処理システムによれば、複数のネットワーク構成用の電子機器が同一のネットワーク上に接続される場合であって、一以上の情報処理装置と情報提供管理手段とが通信手段により接続され、情報提供管理手段では、情報処理装置から転送される情報を処理し表示情報を含む電子情報内容を提供するようになされる。これを前提にして、当該システムへの参加時等に情報提供管理手段又は情報処理装置において、当該情報処理装置の入力操作機能を利用して使用者本人を特定するための認証処理がなされる。

【0012】例えば、情報提供管理手段において使用者本人を認証処理する場合であって、予め情報処理装置から情報提供管理手段へ使用者の顔画像情報及び個人情報登録請求される。情報提供管理手段では情報処理装置によって登録請求された使用者の顔画像情報に個人情報を付加して管理すると共に、使用者の情報処理装置に対して登録済みを示すキー情報が配信される。

【0013】以後、情報提供管理手段に対して情報処理装置の入力操作機能を利用してキー情報が提示されたとき、情報提供管理手段ではキー情報に基づいて顔画像情報から個人情報を読み出し、ここで読み出された個人情報と提示された個人情報とを比較照合して本人を認証するようになされる。

【0014】従って、顔画像情報から読み出した個人情報と、使用者から提示された個人情報とが一致した場合は当該システムへの参加を許可することができる。また、顔画像情報から読み出した個人情報と、第三者から提示された個人情報とが一致しない場合は当該システムへの参加を拒否することができる。これにより、情報提供管理手段又は情報処理装置において、当該情報提供管理手段を含むネットワーク構成用の電子機器の第三者による不正使用を防止できる。

【0015】本発明に係る第1の情報提供管理装置は少なくとも、使用者の情報処理装置から転送される情報を処理し表示情報を含む電子情報内容を提供する装置であって、情報処理装置から登録請求された使用者の顔画像情報及び個人情報を記憶する記憶手段と、この情報処理装置によって登録請求された使用者の顔画像情報に個人情報を付加して管理すると共に、使用者の情報処理装置に対して登録済みを示すキー情報を配信する制御装置と



を備え、当該制御装置に対して情報処理装置からキー情報が提示されたとき、キー情報に基づいて顔画像情報から個人情報を読み出し、ここで読み出された個人情報と提示された個人情報とを比較照合して本人を認証するようにしたことを特徴とするものである。

【0016】本発明に係る第1の情報提供管理装置によれば、少なくとも、使用者の情報処理装置から転送される情報を処理し表示情報を含む電子情報内容を提供する場合に、記憶手段には情報処理装置から登録請求された使用者の顔画像情報及び個人情報が記憶される。制御装置では使用者の顔画像情報に個人情報を付加して管理すると共に、この使用者の情報処理装置に対して登録済みを示すキー情報が配信される。これを前提にして、当該制御装置に対して情報処理装置からキー情報が提示されると、この制御装置ではキー情報に基づいて顔画像情報から読み出した個人情報と、提示された個人情報とを比較照合して本人を認証するようになされる。

【0017】従って、当該情報提供管理装置において使用者本人を認証処理することができる。これにより、複数のネットワーク構成用の電子機器が同一のネットワーク上に接続される情報処理システムに対して第1の情報提供管理装置を十分応用することができる。

【0018】本発明に係る第2の情報提供管理装置は少なくとも、使用者の情報処理装置から転送される情報を処理し表示情報を含む電子情報内容を提供する装置であって、情報処理装置から登録請求された使用者の顔画像情報及び個人情報を記憶する記憶手段と、この情報処理装置によって登録請求された使用者の顔画像情報に個人情報を付加した使用者顔画像情報を作成すると共に、使用者顔画像情報及び登録済みを示すキー情報を使用者の情報処理装置に配信する制御装置とを備えることを特徴とするものである。

【0019】本発明に係る第2の情報提供管理装置によれば、少なくとも、使用者の情報処理装置から転送される情報を処理し表示情報を含む電子情報内容を提供する場合に、記憶手段には情報処理装置から登録請求された使用者の顔画像情報及び個人情報が記憶される。制御装置では使用者の顔画像情報に個人情報を付加して使用者顔画像情報を作成すると共に、この使用者顔画像情報及び登録済みを示すキー情報が使用者の情報処理装置に配信される。

【0020】従って、当該情報処理装置においてキー情報に基づき使用者顔画像情報から読み出した個人情報と、提示された個人情報とを比較照合して本人を認証することができる。これにより、情報処理装置側で使用者本人を認証できることから、複数のネットワーク構成用の電子機器が同一のネットワーク上に接続される情報処理システムに対して第2の情報提供管理装置を十分応用することができる。

【0021】本発明に係る情報処理装置は使用者本人を

認証するためのキー情報に基づいて任意の情報を処理する装置であって、キー情報を入力する入力手段と、予め取得された使用者顔画像情報及び登録済みを示すキー情報を記憶する記憶手段と、入力手段により入力されたキー情報に基づいて記憶手段から使用者顔画像情報を読み出すと共に使用者顔画像情報から個人情報を読み出し、使用者顔画像情報から読み出された個人情報と入力手段により入力された個人情報とを比較照合して使用者本人を認証する制御装置とを備えることを特徴とするものである。

【0022】本発明に係る情報処理装置によれば、使用者本人を認証するためのキー情報に基づいて任意の情報を処理する場合に、入力手段を使用してキー情報が入力される。予め取得された使用者顔画像情報及び登録済みを示すキー情報が記憶手段に記憶されている。これを前提にして、制御装置ではキー情報に基づいて使用者顔画像情報から個人情報を読み出し、この使用者顔画像情報から読み出された個人情報と入力手段により入力された個人情報とを比較照合するようになされる。

【0023】従って、当該情報処理装置において使用者本人を認証することができる。これにより、複数のネットワーク構成用の電子機器が同一のネットワーク上に接続される情報処理システムに対して当該情報処理装置を十分応用することができる。

【0024】本発明に係る情報処理方法は入力操作機能を有して任意の情報を処理する一以上の情報処理系と、少なくとも、情報処理系から転送される情報を処理し表示情報を含む電子情報内容を提供する情報提供管理系とを準備し、情報提供管理系又は情報処理系において、当該情報処理系の入力操作機能を利用して使用者本人を特定するための認証処理をするようにしたことを特徴とするものである。

【0025】本発明に係る情報処理方法によれば、顔画像情報から読み出した個人情報と、使用者から提示された個人情報とが一致した場合は当該システムへの参加を許可することができる。また、顔画像情報から読み出した個人情報と、第三者から提示された個人情報とが一致しない場合は当該システムへの参加を拒否することができる。これにより、情報提供管理系又は情報処理系において、当該情報提供管理系を含むネットワーク構成用の電子機器の第三者による不正使用を防止できる。

【0026】

【発明の実施の形態】続いて、この発明に係るネットワーク情報処理システム、情報提供管理装置、情報処理装置及び情報処理方法の一実施の形態について、図面を参照しながら説明をする。

【0027】(1)実施形態

図1は本発明に係る実施形態としてのネットワーク情報処理システム100の構成例を示すブロック図である。この実施形態では任意の情報を処理する一以上の情報処

理装置と、表示情報を含む電子情報内容を提供する情報提供管理手段とを通信手段により接続し、情報提供管理手段又は情報処理装置において、当該情報処理装置の入力操作機能を利用して使用者本人を特定するための認証処理をし、顔画像情報から読み出した個人情報と、使用者から提示された個人情報とが一致しない場合は当該システムへの参加を拒否できるようにすると共に、当該情報提供管理手段を含むネットワーク構成用の電子機器の第三者による不正使用を防止できるようにしたものである。

【0028】図1に示すネットワーク情報処理システムは、複数のネットワーク構成用の電子機器が同一のネットワーク上に接続される情報処理システムであり、ネットワーク会議システムや、ネットワーク教育システム、ネットワークゲームシステム等に適用して好適なものである。

【0029】当該システム100は特定の領域又は会議室等の特定の場所に情報提供管理手段10（情報提供管理系I）を配置すると共に、その特定の領域又は特定の場所内に一以上の情報処理装置1（情報処理系II）を準備し、この情報提供管理手段10と各々の情報処理装置1とを通信手段4により接続し、これらの情報処理装置1から操作指示に基づいて情報提供管理手段10を遠隔制御するようになされる。情報提供管理手段10は他のネットワーク情報処理システムと接続して使用してもよい。遠隔地間会議システム等を構築することができる。

【0030】このシステム100では情報提供管理手段10又は情報処理装置1において、当該情報処理装置1の入力操作機能を利用して使用者本人を特定するための認証処理をするようにした。例えば、情報提供管理手段10では使用者顔画像情報D0を作成するようになされる。使用者顔画像情報D0とは情報処理装置1によって登録請求された使用者の顔画像情報D1に個人情報D2を付加したものをいう。個人情報D2とは、使用者の名前、社員番号、メールアドレス、電話番号等をいう。

【0031】このシステム100で使用者顔画像情報D0は特定の管理者によって作成され、情報提供管理手段10等へ登録し及び使用者の情報処理装置1に発行するようになされる。発行先立ち、情報提供管理手段10では使用者の顔画像内に本人を特定する個人情報D2を重畳し、使用時には顔画像内に重畳された個人情報D2を読み出して当該使用者本人を認証するようになされる。こうすることで、第三者が容易に使用者顔画像情報D0を不正使用することができなくなる。

【0032】情報処理装置1はキー情報IDに基づいて任意の情報を処理する装置である。キー情報IDには使用者本人を認証するためパスワードが使用される。情報処理装置1には入力手段の一例となるキーボード14及びマウス8が備えられている。キーボード14はキー情報IDや、グループ識別情報等を入力する際に使用され

る。当該システム100を終了する際にはエグジットキー等を押下するようになされる。マウス8はファイル転送時等においてポインタ操作する際に使用される。キーボード14及びマウス8には制御装置13が接続されている。

【0033】この制御装置13には記憶手段12が接続され、予め取得された使用者顔画像情報D0及び登録済みを示すキー情報IDを記憶するようになされる。制御装置13ではキーボード14により入力されたキー情報IDに基づいて記憶手段12から使用者顔画像情報D0を読み出すと共に使用者顔画像情報D0から個人情報D2を読み出し、使用者顔画像情報D0から読み出された個人情報D2とキーボード14により入力された個人情報D2とを比較照合して使用者本人を認証するようになされる。

【0034】この制御装置13には表示手段の一例となる液晶ディスプレイ11が接続されており、使用者の顔画像を表示するようになされる。液晶ディスプレイ11には入力操作機能の一例となるグラフィックユーザインタフェース（以下でGUI機能という）を有しており、このGUI機能及びマウス操作機能を利用して任意の情報を処理するようになされる。

【0035】液晶ディスプレイ11には使用者の顔画像に付加された個人情報D2をGUI機能を利用して表示される。ここでGUI機能を利用した入力操作とはマウス8の右クリック等の操作をいう。このようにすると、他の参加者が該当する使用者顔画像の所有者の個人情報D2を容易に確認することができる。このシステム100で使用者が未認証である場合は、液晶ディスプレイ11には当該使用者が未認証である旨の表示がなされる。

【0036】情報処理装置1には持ち運び便利なノート型のパーソナルコンピュータが使用される。電子会議システム等に参加する場合には専用のアプリケーション（クライアントGUIプログラム等）が予め情報処理装置1にインストールされる。情報提供管理手段10では少なくとも、この情報処理装置1から転送される情報を処理し表示情報を含む電子情報内容を提供するようになされる。

【0037】なお、システム100で情報処理装置1を不特定多数の利用者により共通に操作する場合は予め情報提供管理手段10へ登録しておいた自分の使用者顔画像情報D0を当該情報処理装置1にダウンロードして使用するようになされる。

【0038】続いて、本発明に係る実施形態としての情報処理方法について当該システム100における認証処理例について説明をする。この実施形態ではGUI機能を有して任意の情報を処理する一以上の情報処理系IIと、少なくとも、情報処理系IIから転送される情報を処理し表示情報を含む電子情報内容を提供する情報提供管理系Iとを準備し、情報提供管理系I又は情報処理系II



において、当該情報処理系IIのGUI機能を利用して使用者本人を特定するための認証処理をする場合を前提とする。

【0039】このシステム100では

① 情報提供管理系Iにおいて、当該情報処理系IIのGUI機能を利用して使用者本人を特定するための認証処理をする場合、及び、

② 情報処理系IIにおいて、当該情報処理系IIのGUI機能を利用して使用者本人を特定するための認証処理をする場合について分けて説明をする。もちろん、情報処理装置1と情報提供管理手段10とが通信手段4により接続されていることが好ましいが、登録済みを示すキー情報IDは記憶媒体（例えばCD-ROM等）を利用して配布してもよい。

【0040】〔情報提供管理系Iで認証処理をする場合①〕図2は、情報提供管理系Iにおける認証例を示すフローチャートである。このシステム100で情報提供管理手段10において使用者本人を認証処理する場合を前提とする。これを処理条件にして、当該情報提供管理手段10では図2に示すステップA2で使用者の情報処理装置1からの顔画像情報D1及び個人情報D2の登録請求が待たれる。

【0041】この登録請求が有った場合はステップA2に移行して情報提供管理手段10では情報処理装置1によって登録請求された使用者の顔画像情報D1に個人情報D2を付加して管理するようになされる。このとき、個人情報D2には情報提供管理手段10を含むネットワーク構成用の電子機器を操作できる範囲を示した操作権情報が付加される。こうすると使用者がネットワーク会議参加時等において、マウス操作できる範囲を限定することができる。そして、ステップA3に移行して使用者の情報処理装置1に対して登録済みを示すキー情報IDが配信される。その後、ステップA8に移行する。

【0042】また、ステップA1で登録請求が無い場合はステップA4に移行して、情報処理装置1から当該情報提供管理手段10へ使用者のキー情報ID及び個人情報D2の提示が有ったかがチェックされる。使用者からの認証要求を監視するためである。この提示がない場合はステップA1に戻る。

【0043】使用者の情報処理装置1では登録済みを示すキー情報IDの配信を受けた後は、情報提供管理手段10に対してGUI機能を利用してキー情報IDが提示される。このときには、情報処理装置1と情報提供管理手段10とが通信手段4により接続されていることが前提となる。これを処理条件にして、情報処理装置1に対してステップA4で使用者からの認証要求が有った場合は、ステップA5に移行して情報提供管理手段10ではキー情報IDに基づいて顔画像情報D1から個人情報D2が読み出され、ここで読み出された個人情報D2と提示された個人情報D2とを比較照合して本人を認証する

ようになされる。

【0044】従って、顔画像情報D1から読み出した個人情報D2と、使用者から提示された個人情報D2とが一致した場合は当該システムへの参加を許可することができる。また、顔画像情報D1から読み出した個人情報D2と、第三者から提示されたような個人情報D2とが一致しない場合は当該システムへの参加を拒否することができる。これにより、情報提供管理手段10において、当該情報提供管理手段10を含むネットワーク構成用の電子機器の第三者による不正使用を防止できる。

【0045】〔情報処理系IIで認証処理をする場合②〕図3A及びBは情報処理系IIにおける認証例を示すフローチャートである。このシステム100で情報処理装置1において使用者本人を認証処理する場合を前提とする。

【0046】これを処理条件にして情報提供管理手段10では、図3Aに示すフローチャートのステップB1で使用者の情報処理装置1からの顔画像情報D1及び個人情報D2の登録請求が待たれる。

【0047】この登録請求が有った場合は、ステップB2に移行して情報提供管理手段10では情報処理装置1によって登録請求された使用者の顔画像情報D1に個人情報D2を付加した使用者顔画像情報D0を作成する。個人情報D2はキー情報IDによって復号可能な情報に暗号化され、暗号化後の個人情報D2を使用者の顔画像内の上下の所定ラインを表示する画像表示情報に重畳するようになされる。こうすると、個人情報D2を容易に復号、改ざんできないようにすることができる。

【0048】そして、ステップB3に移行して情報提供管理手段10から使用者の情報処理装置1に対して使用者顔画像情報D0及び登録済みを示すキー情報IDが配信される。このとき、使用者顔画像情報D0及び登録済みを示すキー情報IDはCD-ROM等の記憶媒体を利用して配布してもよい。

【0049】また、情報処理装置1では図3Bに示すフローチャートのステップC1で使用者顔画像情報D0＋登録済みを示すキー情報IDを受信（インストール）する。その後、例えば、情報処理装置1と情報提供管理手段10とを通信手段4により接続してネットワーク電子会議システム等を構築する場合に、ステップC2に移行して当該情報処理装置1では当該GUI機能を利用したキー情報ID乃至個人情報D2が入力されるのを待つ。

【0050】キー情報ID乃至個人情報D2が入力された場合は、ステップC3に移行して情報処理装置1ではキー情報IDに基づいて使用者顔画像情報D0から個人情報D2が読み出される。ここで読み出された個人情報D2はステップC4で先に提示された個人情報D2とを比較照合され、本人を認証するようになされる。

【0051】このシステム100で使用者顔画像情報D0を構成する画像表示情報にはチェック情報が含まれ、

使用者の認証時にチェック情報に基づいて画像表示情報の符号ビットを加算し、符号ビットを加算した加算結果とチェック情報による期待加算結果とを比較照合するようになされる。

【0052】そして、比較照合結果がステップC5で液晶ディスプレイ11に表示される。上述の比較照合の結果で、符号ビットを加算した加算結果とチェック情報による加算結果とが一致しない場合は、当該システムへの使用者の参加を拒否するようになされる。又は、情報提供管理手段10を含むネットワーク構成用の電子機器の使用権利が制限される。この際の制限に関しては、会議に参加できないようにする、その使用者が未認証であることが他の参加者に容易にわかるような使用者顔画像情報D0の表示での参加、かつ、チャットやファイル転送等のサービスが受けられない等、使用権を制限するようになされる。

【0053】このように、本発明に係る実施形態としてのネットワーク情報処理システム100によれば、当該システムへの参加時等に情報提供管理手段10又は情報処理装置1において、当該情報処理装置1のGUI機能を利用して使用者本人を特定するための認証処理がなされる。

【0054】従って、顔画像情報D1から読み出した個人情報D2と、使用者から提示された個人情報D2とが一致した場合は当該システムへの参加を許可することができる。また、顔画像情報D1から読み出した個人情報D2と、第三者から提示された個人情報D2とが一致しない場合は当該システムへの参加を拒否することができる。これにより、情報提供管理手段10又は情報処理装置1において、当該情報提供管理手段10を含むネットワーク構成用の電子機器の第三者による不正使用を防止できる。

#### 【0055】(2) 実施例

図4は本発明に係る実施例としての遠隔地間電子会議システム102の構成例を示すイメージ図である。この実施例ではネットワーク情報処理システムの一例となる遠隔地間電子会議システム102を構築し、情報提供管理手段で予め使用者顔画像情報D0を作成し、これを個々の使用者の情報処理装置に配布し、会議システム参加時にユーザの認証するようにしたものである。

【0056】図4に示す遠隔地間電子会議システム102はローカル側の情報処理システム#1と、リモート側の情報処理システム#2とが通信手段の一例となるHUB(集線接続器)9A、9Bやゲートウェイ40、通信ケーブル40A、40B、41等を通じて接続され、これらの情報処理システム#1、#2間において、ユーザ情報を相互に交換するようにしたものである。

【0057】ローカル側の情報処理システム#1には情報提供管理手段の一例となるプレゼンテーション装置10Aが備えられ、2台のノートパソコンPCi(i=

1, 2)が準備される。プレゼンテーション装置10Aは情報提供管理系Iを構成し、ノートパソコンPCiは情報処理系IIを構成する。プレゼンテーション装置10Aと各々のノートパソコンPC1, PC2とは無線LAN通信方式により接続して使用される。ノートパソコンPC1, PC2のGUI機能を利用してプレゼンテーション装置10Aを遠隔制御するようになされる。

【0058】プレゼンテーション装置10Aはプロジェクタ2A及びコミュニケータ3Aを有している。コミュニケータ3Aはグローバルアドレス(43. 2. 57. 11)及びIPアドレス(192. 168. 0. 1)を有しており、ノートパソコンPC1, PC2から遠隔操作指示に基づいてプロジェクタ2Aを含む電子情報処理を支援するようになされる。

【0059】コミュニケータ3Aはパーソナルコンピュータ機能を有しており、ノートパソコンPC1, PC2の入力操作機能によって情報処理をするようになされる。ノートパソコンPC1はLocal1であり、ノートパソコンPC2はLocal2である。コミュニケータ3Aはローカル側のHUB9に接続され、通信ケーブル40A、ゲートウェイ40及び通信ケーブル41を通じてリモート側の情報処理システム#2に接続されている。

【0060】また、リモート側の情報処理システム#2には情報提供管理手段の一例となるプレゼンテーション装置10Bが備えられ、2台のノートパソコンPCi(i=3, 4)が準備される。プレゼンテーション装置10Bも情報提供管理系Iを構成し、ノートパソコンPCiも情報処理系IIを構成する。プレゼンテーション装置10Bと各々のノートパソコンPC3, PC4とは無線LAN通信方式により接続して使用される。ノートパソコンPC3, PC4のGUI機能を利用してプレゼンテーション装置10Bを遠隔制御するようになされる。

【0061】プレゼンテーション装置10Bはプロジェクタ2B及びコミュニケータ3Bを有している。コミュニケータ3Bはグローバルアドレス(43. 0. 21. 121)及びIPアドレス(192. 168. 0. 1)を有しており、ノートパソコンPC3, PC4から遠隔操作指示に基づいてプロジェクタ2Bを含む電子情報処理を支援するようになされる。コミュニケータ3Bもパーソナルコンピュータ機能を有しており、ノートパソコンPC3, PC4の入力操作機能によって情報処理をするようになされる。ノートパソコンPC3はRemote1であり、ノートパソコンPC4はRemote2である。

【0062】コミュニケータ3Bはリモート側のHUB9に接続され、通信ケーブル40B、ゲートウェイ40及び通信ケーブル41を通じてローカル側の情報処理システム#1に接続されている。この電子会議システム102ではローカル側のコミュニケータ3Aはユーザ情報

として以下の参加者情報、つまり、参加者のノートパソコンPCiのIPアドレスを管理する。その参加者情報として、

<User名>	<IPアドレス>
Local 1	192. 168. 0. 129
Local 2	192. 168. 0. 214

を管理するようになされる。同様に、リモート側のコミュニケータ3Bはユーザ情報として以下の参加者情報、つまり、参加者のノートパソコンPCiのIPアドレスを管理する。その参加者情報としては、

<User名>	<IPアドレス>
Remote 1	192. 168. 0. 84
Remote 2	192. 168. 0. 53

を管理するようになされる。そして、ローカル側とリモート側とを接続した時は、これらの参加者情報をコミュニケータ3A及び3B間で交換し合うようになされる。

【0063】各々のノートパソコンPCiはキー情報の一例となるユーザキーIDに基づいて任意の情報を処理する装置である。ユーザキーIDは使用者本人を認証するためパスワード等である。会議参加時にはユーザキーIDに基づいて使用者顔画像情報D0の一例となるユーザアイコン画像情報（以下で単にユーザアイコン画像という）から個人情報の一例となるユーザ情報（User Information）D2を読み出し、このユーザアイコン画像から読み出されたユーザ情報D2とキーボード14により入力されたユーザ情報D2とを比較照合するようになされる。従って、当該ノートパソコンPCiにおいて使用者本人を認証することができる（図1参照）。

【0064】続いて、コミュニケータ3の内部構成例について説明をする。図5はコミュニケータ3A等の内部構成例を示すブロック図である。コミュニケータ3Bについてはコミュニケータ3Aと同様であるのでその説明を省略する。図5に示すコミュニケータ3Aはパソコン機能を有しており、ノートパソコンPCiのマウス操作によって情報処理をするものである。使用者のノートパソコンPCiから転送される情報を処理し表示情報を含む電子情報内容を提供するようになされる。

【0065】コミュニケータ3Aはデータバス36を有しており、このデータバス36にはディスプレイアダプタ31、CPU32、ワーク用のRAM33、データ格納装置34、ネットアダプタ35等が接続される。

【0066】ディスプレイアダプタ31はプレゼンテーション用の資料を処理して、RGB信号を作成する機能を有している。このプレゼンテーション用の資料に基づくRGB信号はプロジェクト2A等に出力される。ワーク用のRAM33はプライベートIPアドレスやプレゼンテーション用の資料に係る転送情報を一時記憶するようになされる。

【0067】データ格納装置34は図示しない記憶手段

の一例となるハードディスク（HDD）、ROM及びRAMから構成されている。ハードディスクには少なくとも、ノートパソコンPCiから登録請求された使用者の顔画像情報D1及びユーザ情報D2を記憶するようになされる。この他にプレゼンテーション用の資料を格納するようになされる。ROMには電子会議システムを支援するための制御プログラム（以下システム支援制御プログラムという）が記述されている。システム支援制御プログラムはCPU32を動作させるための基本ソフトウェアやプレゼンテーションデータを処理するプログラムから構成されている。

【0068】ネットアダプタ35ではノートパソコンPCiからプレゼンテーションデータや各種コマンドの受信を行うようになされる。CPU32は制御装置の一例であり、システム支援制御プログラムに基づいてディスプレイアダプタ31、ワーク用のRAM33、データ格納装置34、ネットアダプタ35等の入出力を制御するようになされる。

【0069】例えば、CPU32では使用者のノートパソコンPCiによって登録請求された使用者の顔画像情報D1にユーザ情報D2を付加して管理すると共に、その使用者のノートパソコンPCiに対して登録済みを示すユーザキーIDを配信するようになされる。

【0070】そして、当該コミュニケータ3AのCPU32に対してノートパソコンPCiからユーザキーIDが提示されたとき、ユーザキーIDに基づいて顔画像情報D1からユーザ情報D2を読み出し、ここで読み出されたユーザ情報D2と提示されたユーザ情報D2とを比較照合して本人を認証するようになされる。従って、情報提供管理系Iで認証処理をする①の場合に相当し、当該プレゼンテーション装置10A等において使用者本人を認証処理することができる（第1の情報提供管理装置）。

【0071】また、情報処理系IIで認証処理をする②の場合には、少なくとも、データ格納装置34にはノートパソコンPCiから登録請求された使用者の顔画像情報D1及びユーザ情報D2が記憶される。CPU32ではユーザアイコン作成登録プログラム等を使用して、使用者の顔画像情報D1にユーザ情報D2を付加してユーザアイコン画像を作成すると共に、このユーザアイコン画像及び登録済みを示すユーザキーIDが使用者のノートパソコンPCiに配信される（第2の情報提供管理装置）。

【0072】従って、当該ノートパソコンPCiにおいてユーザキーIDに基づきユーザアイコン画像から読み出したユーザ情報D2と、提示されたユーザ情報D2とを比較照合して本人を認証することができる。これにより、ノートパソコンPCi側で使用者本人を認証できる。

【0073】図6は使用者固定データUCDのフォーマ

ット例を示すイメージ図である。この例では情報処理系IIで認証処理をする②の場合を想定する。図6に示すデータフォーマット例によれば、42 Bytesのユーザ情報D2に対して、チェック情報の一例となる3 Bytesのチェックサムが付加され、45 Bytesの使用

者固定データ (User Confirm Data: UCD) がCPU32によって作成される。42 Bytesのユーザ情報D2は暗号化の対象範囲となる。

【0074】この使用者固定データUCDの先頭の2 BytesにはヘッダーID (Header ID) が記述される。ヘッダーIDにはヘッダコード (固定値=0xEC) が記述され、通常の参加又はゲスト (Guest) 参加の区別がなされる。なお、ゲストの場合は0x00が記述される。ヘッダコードの後方にはライトコード (Right Code) が記述される。ライトコードには管理者が登録時に設定した会議参加中の操作権に関する内容が記述される。

【0075】ライトコードは8ビットで表示される [bit7→bit0, 7:0]。許可内容は「1」又は「0」であり、「1」で許可を示す。bit7及びbit6は予備 (Reserved:0) であり、bit5にはコミュニケータのステップアップ設定権の許可内容が記述される。bit4にはプレゼンテーション (Presentation) 操作権の許可内容が記述される。bit3にはプロジェクタ (Viewer) へのファイル転送操作の許可内容が記述される。bit2にはプロジェクタの表示切り替え操作の許可内容が記述される。bit1にはチャット操作の許可内容が記述される。bit0にはファイル転送操作の許可内容が記述される。

【0076】ヘッダーIDの後方にはユーザ名 (User Name) の記述欄として12 Bytesが割り当\*

UCD [44:0] [7:00]  
= (Header ID [1:0] [7:0]、  
User Name [11:00] [7:00]、  
Full Name [19:0] [7:00]  
User ID [7:0] [7:0]  
Check Sum [2:0] [7:0] ..... (2)

となる。

【0080】また、yライン目の左からx番目のR、

Rorg [x] [y] [7:0]  
Gorg [x] [y] [7:0]  
Borg [x] [y] [7:0] ..... (3)

【0081】更に、y=55ライン目の左からx番目のR、G、B色の画素データの使用者固定データUCDの

R [x] [55] [7:0]  
= (Rorg [x] [7:1]、UCD [x] [7])  
G [x] [55] [7:0]  
= (Gorg [x] [7:1]、UCD [x] [6])  
B [x] [55] [7:0]

\*てられる。ユーザ名は英数字で最大12文字まで記述可能となされている。ユーザ名の後方にはフルネーム (Full Name) の記述欄として20 Bytesが割り当てられる。フルネームは英数字で最大20文字まで記述可能となされている。フルネームの後方にはユーザID (User ID) の記述欄として8 Bytesが割り当てられる。ユーザIDは英数字で最大8文字まで記述可能となされている。ユーザ情報D2の後方には3 Bytesのチェックサム (Check Sum) が記述される。

【0077】図7は顔画像ファイルへの重畳 (埋め込み) 例を示すイメージ図である。この例ではユーザの顔画像が予め準備される。ユーザの顔部位を予めデジタルカメラで撮影して得た顔画像データ (画像表示情報) が使用される。ユーザアイコン画面Qの大きさは縦×横=55画素×45画素であり、ユーザの顔画像は55×45画素 (Pixel) 内に収まる程度の24ビットマップ (Bitmap) 画像から成る。このビットマップ画像の1画素はR (赤色:1 byte)、G (緑色:1 byte)、B (青色:1 byte) の3 bytesで構成される。

【0078】この例で暗号化後の使用者固定データUCDは使用者の顔画像内の上下の1ラインを表示する画像表示データの下位ビットに重畳 (記述) される。使用者固定データUCDはユーザ情報D2+チェックサムから構成される。

【0079】この例では使用者固定データUCDの最初からxバイト目を次式 (1) のように定義する。

UCD [x] [7:0] ..... (1)

ユーザの顔画像の大きさが縦×横=55画素×45画素であることから、図6に示したフォーマット例により次式 (2)、すなわち、

※G、B色の画素データに関してオリジナルデータを次の

※40 式 (3) ように定義する。

挿入後のデータを次の式 (4) のように定義する。

21

22

$$= (\text{Borg}[x][7:2], \text{UCD}[x][5:4]) \cdots (4)$$

【0082】また、 $y=1$ ライン目の左から $x$ 番目の \*挿入後のデータを次の式(5)のように定義する。  
R, G, B色の画素データの使用者固定データUCDの\*

$$\begin{aligned} & \text{R}[x][1][7:0] \\ &= (\text{R}[x][7:1], \text{UCD}[x][3]) \\ & \text{G}[x][1][7:0] \\ &= (\text{G}[x][7:1], \text{UCD}[x][2]) \\ & \text{B}[x][1][7:0] \\ &= (\text{B}[x][7:2], \text{UCD}[x][1:0]) \cdots (5) \end{aligned}$$

【0083】この例では3bytesのチェックサムに 10※(6)のように定義する。  
については、ビットマップ画像のR、G、Bについて次式※

$$\begin{aligned} \text{Check Sum}[2][7:0] &= \text{CSR}[7:0] \\ \text{Check Sum}[1][7:0] &= \text{CSG}[7:0] \\ \text{Check Sum}[0][7:0] &= \text{CSB}[7:0] \cdots (6) \end{aligned}$$

【0084】このビットマップ画像のR、G、B色に係 ★ットを加算するチェックサムは次式(7)のように定義  
る $x$ 方向に符号ビットを加算し、 $y$ ライン方向に符号ビ★ する。

$$\begin{aligned} & \text{CSR}[7:0] \\ &= \text{R}[x][y][7:0] \text{の総和} (1 \leftarrow x \leftarrow 42, 1 \leftarrow y \leftarrow 55) \\ & \text{CSG}[7:0] \\ &= \text{G}[x][y][7:0] \text{の総和} (1 \leftarrow x \leftarrow 42, 1 \leftarrow y \leftarrow 55) \\ & \text{CSB}[7:0] \\ &= \text{B}[x][y][7:0] \text{の総和} (1 \leftarrow x \leftarrow 42, 1 \leftarrow y \leftarrow 55) \\ & \cdots (7) \end{aligned}$$

【0085】続いて、ユーザアイコン画像の作成例について説明をする。図8はユーザアイコン画像の作成例を示すフローチャートである。この実施例でユーザが対象となるネットワーク電子会議システムや、ネットワーク教育システム等を利用する場合に、予めシステム管理者にユーザアイコン画像を作成してもらいこれを登録するようになされる。

【0086】この例ではユーザアイコン画像をシステム管理者のパーソナルコンピュータ（以下でパソコンという）等を使用して作成する場合を想定する。もちろん、システム管理者がコミュニケータ3A等を管理するのであれば、コミュニケータ3A等で作成してもよい。いずれも、会議前日に登録を済ませておくことが好ましい。

【0087】これを処理条件にしてシステム管理者のパソコン又はコミュニケータ3A等では、図8に示すフローチャートのステップE1で使用者のノートパソコンPCiからの顔画像情報D1及びユーザ情報D2のアイコン登録請求が待たれる。

【0088】このアイコン登録請求が有った場合は、ステップE2に移行してコミュニケータ3A等ではノートパソコンPCiによって登録請求された使用者の顔画像情報D1にユーザ情報D2を付加したユーザアイコン画像を作成する。なお、ステップE2～E8はシステム管理者におけるアイコン作成登録プログラムが使用される。

【0089】このとき、管理者はユーザから顔写真、ユーザキーID（キー情報）、ユーザ名、フルネーム、ユ

ーザIDを入手する。ここで、ユーザIDには社員番号、電話番号、部課コードなどが使用される。管理者はこれらの情報に加え、アイコン登録請求者（ユーザ）にシステム102上、どこまで操作権を許可するかを設定する。この設定は使用者固定データUCDのライトコードにその内容を記述することで制限するようになされる。

【0090】この際に、システム管理者のパソコン又はコミュニケータ3A等ではヘッダーコード（2bytes：0xEC\*\*）、\*\*はライトコード（1byte）、ユーザ名（12bytes：英数字12文字）、フルネーム（20bytes：英数字20文字）及びユーザID（8bytes：英数字8文字）で構成されるユーザ情報D2（42bytes）が作成される。

【0091】その後、ステップE3でユーザ情報D2はユーザキーID（パスワード）に基づいて復号可能な暗号化される。暗号アルゴリズムには共有鍵方式（DESなど）が使用される。ユーザは、会議参加時等において、当該システム102にログインするときにこのユーザキーIDを入力して正規に登録されたユーザであることをチェックされる。

【0092】そして、ステップE4に移行して暗号化後のユーザ情報D2は、図7に示したユーザアイコン画面Q内に重畳される。ユーザ情報D2は顔画像が劣化しないように、かつ目立たない位置に埋め込まれる。この例では、ユーザアイコン画面Qの上下1ラインを表示するR、G、B色の画像データの下位ビットに埋め込まれ

30

40

50

る。こうすると、ユーザ情報D2を容易に復号、改ざんできないようにすることができる。

【0093】その後、ユーザアイコン画面Qに埋め込まれた画像データに対する、R、G、B色のそれぞれのチェックサムをステップE5で計算し、R、G、B色に係るチェックサムをステップE6で再度、顔画像データに埋め込む。顔画像データが改ざんされた場合は、このチェックサムのチェック機能で判別することができる。

【0094】そして、ステップE7では作成されたファイル名は、ユーザ名に関連した名前登録される。システム管理者のパソコンや、当該システム102でコミュニケーション3A等をサーバ装置としたとき、このコミュニケーション3A等に登録する。このようにすることで、ステップE8で常にコミュニケーション3A等からユーザアイコン画像及び登録済みを示すユーザキーIDを参照又は発行（配信）できるようになる。

【0095】この場合、常にサーバ装置等にアクセスできる環境でしかシステム102が稼働できなくなってしまうため、そのような場合には、アイコン登録請求者に対してCD-ROM等の記憶媒体にユーザアイコン画像を記録し手渡して発行し、使用者のノートパソコンPCi上に置くことも可能である。

【0096】図9はノートパソコンPCiにおける起動時のGUI操作画面（以下でGUI起動時画面という）P0の表示例を示すイメージ図である。図9に示すGUI起動時画面P0は起動時にノートパソコンPC1に表示されるものであり、クライアントGUIプログラムに基づく表示例である。GUI起動時画面P0では2分割表示方式が採られる。当該画面P0の左側にはGUI操作画面（以下でコントロール画面という）P1が表示され、画面右側にはアテンディ画面P2が表示される。この例で、コントロール画面P1にはスクリーン・スナップモードによる選択画面が表示される。

【0097】コントロール画面P1において、中央にはデバイスアイコン用のエリア21が設けられ、プロジェクト等のアイコンが表示される。このエリア21の上部にはスクリーンスナップモード時の「start」や、「stop」ボタンK0が表示される。その右隣にはアテンディボタンK1が表示され、その上方には「HELP」ボタンK2が表示され、このコントロール画面P1の外枠上部には「閉じる」ボタンK3が表示されている。エリア21の下方には「ファイル・エクスプローラ／ヒストリ」用のタブK4が表示され、このタブK4内にはファイルリストエリア22を表示するようになされる。なお、コントロール画面P1の左側上部には企業イメージのロゴマーク19を表示できるようになされている。

【0098】アテンディ画面P2において、中央にはアテンディユーザリスト用のエリア23が設けられ、会議参加者や、そのノートパソコンPCiのIPアドレス等

がアイコンと共に表示される。このエリア23の上部にはユーザ情報エリア24が設けられ、使用者固定データUCDに基づくユーザアイコン画像が表示される。この他に、ユーザ情報エリア24にはローカル側で特定のノートパソコンPCiのIPアドレス等を表示するようになされる。アテンディ画面P2の右側上部には「チャット」ボタンK5が表示される。また、アテンディ画面P2の下方にはローカルボタンK6、リモートボタンK7及びクリアボタンK8等を表示するようになされる。

10 【0099】図10はアテンディ画面P2におけるユーザアイコン画像の表示例を示すイメージ図である。図10に示すアテンディ画面P2によれば、ユーザ情報エリア24にはユーザアイコン画像が表示される。この例では会議参加が許可されたユーザの顔画像、ユーザ名〇〇〇、当該ノートパソコンPCiのIPアドレスとして43.2.57.193が表示される。なお、アテンディユーザリスト用のエリア23にはRemoteの会議参加者の顔画像、ユーザ名×××、当該ノートパソコンPCiのIPアドレスとして192.168.0.222が表示される。

20 【0100】図11はコントロール画面P1におけるファイル確認画面P11の表示例を示すイメージ図である。図11に示すファイル確認画面P11によれば、不特定多数の使用者、つまり、別の参加者が当該ノートパソコンPCiを使用して会議に参加しようとする場合である。この場合はユーザフォトに関してファイル確認画面P11を開き、ユーザ名×××を入力すると、それに関連した画像ファイルのリストが表示される。

30 【0101】このリストの中からユーザ名×××を選択（クリック）すると、リストの隣の所定の表示領域にRemoteの会議参加者の顔画像が表示される。ユーザ名はファイル名と共にファイルの種類を指定することで当該ノートパソコンPCi内に保存される。Remote側の会議参加者がローカル側に出向して会議に参加する場合が考えられるためである。

40 【0102】図12はコントロール画面P1におけるセットアップ画面P12の表示例を示すイメージ図である。図12に示すセットアップ画面P12はファイル確認画面P11でユーザ名×××を選択することで表示切替されたアイコン画面である。このセットアップ画面P12にはUSER NAME ×××や、USER PHOTO (45×55 pixels) として、Remoteの会議参加者の顔画像が表示されると共に、USER KEYが表示される。USER KEYにはパスワード「\*\*\*\*\*」を入力するようになされる。セットアップ画面P12にはこの他に閲覧キー（BROWSE）K9や、OKキーK10やキャンセルキーK11が表示される。パスワードが正しければ、Remoteの会議参加者がローカル側の会議に参加できるようになる。



【0103】図13はアテンディ画面P2における制限付きユーザアイコン画像の表示例を示すイメージ図である。図13に示すアテンディ画面P2によれば、ユーザ情報エリア24には制限付きユーザアイコン画像が表示される。この例では会議参加を許可されたが操作権が制限されるゲスト(Guest)、ユーザ名△△△、その者のノートパソコンPCiのIPアドレスとして192.168.0.246が表示される。なお、アテンディユーザリスト用のエリア23にはRemoteの会議参加者の顔画像、ユーザ名×××、当該ノートパソコンPCiのIPアドレスとして192.168.0.222が表示されている。

【0104】図14及び図15は遠隔地間電子会議システム102の会議参加時のノートパソコンPCiにおける処理例(その1、2)を示すフローチャートである。この実施例ではローカル側において、ユーザが会議に参加する場合の流れを示している。例えば、ノートパソコンPCiとコミュニケータ3A等とを通信手段4により接続して遠隔地間電子会議システム102等に参加する場合を想定する。

【0105】この例ではいずれの使用者のユーザアイコン画像+登録済みを示すユーザキーIDは予め当該ノートパソコンPCiにインストールされているものとする。このシステム102でユーザアイコン画像を構成する画像表示情報にはチェック情報(Check Sum)が含まれ、ユーザの認証時にチェック情報に基づいて本人を認証する場合を例に挙げる。これを処理条件にして、前回のユーザが今回も当該ノートパソコンPCiを使用する場合及び、リモート側の使用者がローカル側に出向してこのPCiを使用する場合に分けて説明をする。なお、ゲストの場合はリモート側で既にユーザアイコン画像が登録されている場合を想定する。

【0106】[前回のユーザが今回も当該PCiを使用する場合] 前回のユーザが今回も当該電子会議システム102に参加する場合は、既にセットアップが済んでいる。そして、ノートパソコンPCiでは図14に示すフローチャートのステップF1でクライアントGUIプログラムが起動されると、図9に示したようなGUI起動時画面P0が液晶ディスプレイ11に表示される。

【0107】ここでステップF2で当該ノートパソコンPCiでは前回と同じユーザ名か否かによって制御を分岐するようになるが、今回、ノートパソコンPCiを使用するユーザが前回の使用した人と同じであることから、ステップF5に移行して自分のユーザ名とアイコン画像が表示される。このとき、図10に示すアテンディ画面P2によれば、ユーザ情報エリア24にはユーザアイコン画像が表示される。この例では会議参加が許可されたユーザの顔画像、ユーザ名〇〇〇、当該ノートパソコンPCiのIPアドレスとして43.2.57.193が表示される。

【0108】そして、ステップF6で当該ノートパソコンPCiではGUI機能を利用してユーザキーID乃至ユーザ情報D2が入力される。ここでユーザキーID及びユーザ情報D2が入力されると、ステップF7～ステップF11、F14で42bitsのユーザ情報D2が確認される。

【0109】この例ではステップF7でノートパソコンPCiではユーザキーIDに基づいてユーザアイコン画像からユーザ情報D2及びチェック情報が読出(切り出)される。チェックサムの整合性を確認するためである。

【0110】このとき、上述した式(7)に基づいてビットマップ画像(画像表示情報)のR、G、B色に係るx方向に符号ビットが加算され、yライン方向に符号ビットが加算される。このチェックサムの計算によって、符号ビットを加算した加算結果とチェック情報による期待加算結果とを比較照合するようになされる。この比較照合の結果で、符号ビットを加算した加算結果とチェック情報による加算結果とが一致しない場合は照合結果が不備(NG)としてステップF14に移行する。

【0111】この比較照合が良好(OK)の場合はステップF9に移行してユーザアイコン画像に埋め込まれたユーザ情報D2が復号化される。そして、ステップF10に移行して復号化後のユーザ情報D2と、先に登録されたユーザ情報D2とが比較照合される。ユーザ名の整合性を確認することで、当該ノートパソコンPCi上でユーザが正規に登録された者であるかが確認することができる。

【0112】更に、ステップF11でヘッダーコードの0xECがチェックされる。ヘッダーコードの整合性を確認することでローカル側での通常の会議参加か、リモート側からの出向によるゲスト参加等を判別するためである。このとき、ライトコードによりシステム102上での操作範囲が決定される。

【0113】これらの比較照合結果は液晶ディスプレイ11に表示するようになされる。ステップF11でヘッダーコードが0xECの場合はローカル側における通常の会議参加なので、ステップF12で当該会議システムへの参加が許容される(図10参照)。そして、ステップF13で当該ノートパソコンPCiでは会議終了か否かがチェックされる。この例では当該ノートパソコンPCiにおいてエグジットキーの押下を検出して会議を終了するようになされる。会議を終了しない場合はステップF12に戻って会議が継続される。

【0114】[前回のユーザと異なる使用者(ゲスト)が当該PCiを使用する場合] 例えば、リモート側の使用者が出向してローカル側の電子会議システム102で当該ノートパソコンPCiを使用する場合である。この場合にはその使用者のローカル側でのセットアップが済んでいない。そこで、ノートパソコンPCiでは図14

に示すフローチャートのステップF1でクライアントGUIプログラムが起動されると、図9に示したようなGUI起動時画面P0が液晶ディスプレイ11に表示される。

【0115】ステップF2では前回と同じユーザ名か否かによって制御を分岐するようになるが、今回、ノートパソコンPCiを使用するユーザが前回のユーザと異なることから、ステップF4に移行する。このステップF4でユーザ名×××を入力すると、ユーザフォトに関して図9に示したGUI起動時画面P0から図11に示す

ファイル確認画面P11が開かれ、ユーザ名×××に関連した画像ファイルのリストが表示される。

【0116】このリストの中でユーザ名×××を選択（クリック）すると、リストの隣の所定の表示領域にリモート側で予めセットアップが済んでいる会議参加者の顔画像が表示される。この顔画像に関してはサーバ装置又は自機にすでに登録されているユーザアイコンファイルのうち、ユーザ名の文字列を含むファイル名のビットマップファイルに基づいてリスト表示される。

【0117】そして、ファイル名と共にファイルの種類を指定することで当該ノートパソコンPCi内に保存される。図11示したファイル確認画面P11から図12に示すセットアップ画面P12へ表示切替がなされる。このセットアップ画面P12にはUSER NAME ×××や、USER PHOTO (45×55 pixel) として、Remoteの会議参加者の顔画像が表示されると共に、USER KEYが表示される。USER KEYにはパスワード「\*\*\*\*\*」を入力するようになる。

【0118】これにより、リモート側の使用者のローカル側でのセットアップが終了する。今回のようにリモート側の会議参加者がローカル側に出向して電子会議システム102に参加する場合（ゲスト）が考えられるためである。なお、参加資格のない未登録者の場合はリスト表示がなされない。

【0119】その後、ステップF5で図13に示したアテンディ画面P2にゲストのユーザアイコン画像が表示される。図13に示すアテンディ画面P2によれば、ユーザ情報エリア24には制限付きユーザアイコン画像が表示される。この例では会議参加を許可されたが操作権が制限されるゲスト（Guest）、ユーザ名△△△、その者のノートパソコンPCiのIPアドレスとして192.168.0.246が表示される。

【0120】そして、ステップF6で当該ノートパソコンPCiでは当該GUI機能を利用してユーザキーID乃至ユーザ情報D2が入力される。その後、ステップF7に移行してノートパソコンPCiではユーザキーIDに基づいてユーザアイコン画像からユーザ情報D2及びチェック情報が読み出される。チェックサムの整合性を確認するためである。

【0121】このとき、画像表示情報の符号ビットを加算し、符号ビットを加算した加算結果とチェック情報による期待加算結果とを比較照合するようになる。この比較照合の結果で、符号ビットを加算した加算結果とチェック情報による加算結果とが一致しない場合は照会結果が不備（NG）としてステップF14に移行する。

【0122】この比較照合が良好（OK）の場合はステップF9に移行してユーザアイコン画像に埋め込まれたユーザ情報D2が復号化される。そして、ステップF10に移行して復号化後のユーザ情報D2と、先に登録されたユーザ情報D2とが比較照合される。ユーザ名の整合性を確認することで、当該ノートパソコンPCi上でユーザが正規に登録された者であるかが確認することができる。

【0123】更に、ステップF11でヘッダーコードの0xECがチェックされる。この場合はリモート側からの出向によるゲスト参加であって、ステップF15でヘッダーコードが0x00であることから、ライトコードによりシステム102上での操作範囲が制限される。ステップF15ではコミュニケータ3A等を含むネットワーク構成用の電子機器の使用権利が制限される。この際の制限に関しては、その使用者が未認証であることが他の参加者に容易にわかるようなユーザアイコン画像の表示での参加、かつチャット、ファイル転送等のサービスが受けられない等、使用権を制限するようになる。

【0124】このようにGuestとして操作権が限定された状態で電子会議システムに参加できるようになる（図13参照）。そして、ステップF16で当該ノートパソコンPCiでは会議終了か否かがチェックされる。この例では当該ノートパソコンPCiにおいてエグジットキーの押下を検出して会議を終了するようになる。会議を終了しない場合はステップF15に戻って会議が継続される。

【0125】なお、ステップF8で照会結果がNGの場合、ステップF10でユーザ名が異なっている場合及びヘッダーコードが0xECではない場合はステップF14に移行してヘッダーコードが0x00であるか否かがチェックされる。ヘッダーコードが0x00はもとより何も記述されていない場合は、ステップF17に移行して当該システム101への使用者の参加を拒否するようになる。当該電子会議システム102に参加できないようにするためである。これにより、ユーザアイコン画像を特定のユーザにしか使用できない機構を構築することができる。

【0126】このように、本発明に係る実施例としての遠隔地型電子会議システム102及びその情報処理方法によれば、当該システム102への参加時等にコミュニケータ3A等又はノートパソコンPCiにおいて、当該ノートパソコンPCiのGUI機能を利用して使用者本人を特定するための認証処理がなされる。

【0127】従って、顔画像情報D1から読み出したユーザ情報D2と、使用者から提示されたユーザ情報D2とが一致した場合は当該システム102への参加を許可することができる。また、顔画像情報D1から読み出したユーザ情報D2と、第三者から提示されたユーザ情報D2とが一致しない場合は当該システムへの参加を拒否することができる。これにより、コミュニケータ3A等又はノートパソコンPCiにおいて、当該コミュニケータ3A等を含むネットワーク構成用の電子機器の第三者による不正使用を防止できる。

【0128】この実施例ではネットワーク情報処理システムに関して遠隔地間電子会議システムについて説明したが、これに限られることなく、ネットワーク教育システム、ネットワークゲームシステム等においても、当該情報提供管理系Iを含むネットワーク構成用の電子機器の第三者による不正使用を防止できる。

#### 【0129】

【発明の効果】以上説明したように、本発明に係るネットワーク情報処理システムによれば、任意の情報を処理する一以上の情報処理装置と、表示情報を含む電子情報内容を提供する情報提供管理手段とが通信手段により接続され、情報提供管理手段又は情報処理装置において、当該情報処理装置の入力操作機能を利用して使用者本人を特定するための認証処理をするものである。

【0130】この構成によって、顔画像情報から読み出した個人情報と、使用者から提示された個人情報とが一致した場合は当該システムへの参加を許可することができる。また、顔画像情報から読み出した個人情報と、不正使用者（第三者）から提示された個人情報とが一致しない場合は当該システムへの参加を拒否することができる。従って、情報提供管理手段又は情報処理装置において、当該情報提供管理手段を含むネットワーク構成用の電子機器の第三者による不正使用を防止できる。

【0131】本発明に係る第1の情報提供管理装置によれば、使用者の顔画像情報に個人情報を付加して管理すると共に、この使用者の情報処理装置に対して登録済みを示すキー情報を配信する制御装置を備え、当該制御装置に対して情報処理装置からキー情報が提示されたとき、このキー情報に基づいて顔画像情報から読み出した個人情報と、提示された個人情報とを比較照合して本人を認証するようにしたものである。

【0132】この構成によって、当該情報提供管理装置において使用者本人を認証処理することができる。これにより、複数のネットワーク構成用の電子機器が同一のネットワーク上に接続される情報処理システムに対して当該情報提供管理装置を十分応用することができる。

【0133】本発明に係る第2の情報提供管理装置によれば、使用者の顔画像情報に個人情報を付加して使用者顔画像情報を作成すると共に、この使用者顔画像情報を及び登録済みを示すキー情報を使用しての情報処理装置へ

配信する制御装置を備えるものである。

【0134】この構成によって、当該情報処理装置においてキー情報に基づき使用者顔画像情報から読み出した個人情報と、提示された個人情報とを比較照合して本人を認証することができる。従って、複数のネットワーク構成用の電子機器が同一のネットワーク上に接続される情報処理システムに対して第2の情報提供管理装置を十分応用することができる。

【0135】本発明に係る情報処理装置によれば、キー情報に基づいて任意の情報を処理する場合に使用者本人を認証する制御装置を備え、この制御装置はキー情報に基づいて使用者顔画像情報から個人情報を読み出し、この使用者顔画像情報から読み出された個人情報と入力手段により入力された個人情報とを比較照合するようになされる。

【0136】この構成によって、複数のネットワーク構成用の電子機器が同一のネットワーク上に接続される情報処理システムに対して当該情報処理装置を十分応用することができる。

【0137】本発明に係る情報処理方法によれば、入力操作機能を有して任意の情報を処理する一以上の情報処理系と、少なくとも、情報処理系から転送される情報を処理し表示情報を含む電子情報内容を提供する情報提供管理系とを準備し、これらの情報提供管理系又は情報処理系において、当該情報処理系の入力操作機能を利用して使用者本人を特定するための認証処理をするようになされる。

【0138】この構成によって、顔画像情報から読み出した個人情報と、使用者から提示された個人情報とが一致した場合は当該システムへの参加を許可することができる。また、顔画像情報から読み出した個人情報と、不正使用者（第三者）から提示された個人情報とが一致しない場合は当該システムへの参加を拒否することができる。従って、情報提供管理系又は情報処理系において、当該情報提供管理系を含むネットワーク構成用の電子機器の第三者による不正使用を防止できる。

【0139】この発明はネットワーク会議システムや、ネットワーク教育システム、ネットワークゲームシステム等に適用して極めて好適である。

#### 【図面の簡単な説明】

【図1】本発明に係る実施形態としてのネットワーク情報処理システム100の構成例を示すブロック図である。

【図2】情報提供管理系Iにおける認証例を示すフローチャートである。

【図3】A及びBは情報処理系IIにおける認証例を示すフローチャートである。

【図4】本発明に係る実施例としての遠隔地間電子会議システム102の構成例を示すイメージ図である。

【図5】コミュニケータ3A等の内部構成例を示すブロ

ック図である。

【図 6】使用者固定データ UCD のデータフォーマット例を示すイメージ図である。

【図 7】顔画像ファイル Q への重畳（埋め込み）例を示すイメージ図である。

【図 8】ユーザアイコン画像の作成例を示すフローチャートである。

【図 9】ノートパソコン PC i における GUI 起動時画面 P0 の表示例を示すイメージ図である。

【図 10】アテンディ画面 P2 におけるユーザアイコン 10 画像の表示例を示すイメージ図である。

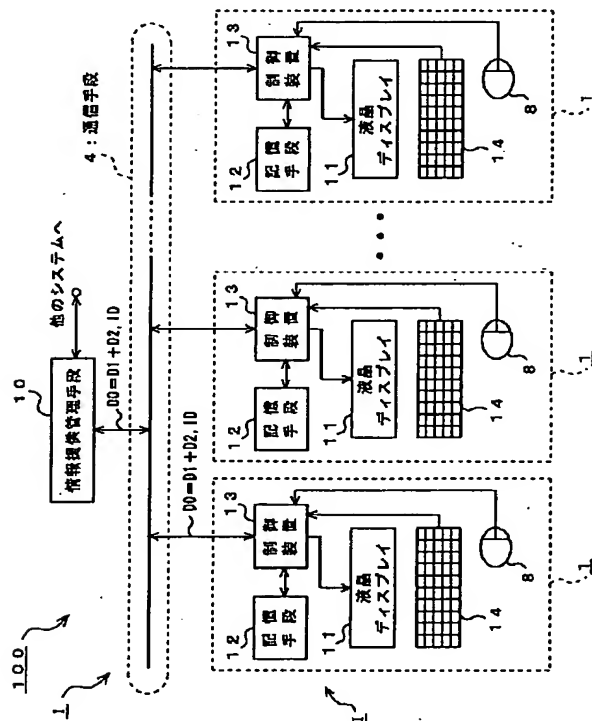
【図 11】コントロール画面 P1 におけるファイル確認画面 P11 の表示例を示すイメージ図である。

【図 12】コントロール画面 P1 におけるセットアップ画面 P12 の表示例を示すイメージ図である。

【図 13】アテンディ画面 P2 における制限付きユーザアイコン画像の表示例を示すイメージ図である。

【図 1】

実施形態としてのネットワーク情報処理システム 100 の構成例



【図 14】遠隔地間電子会議システム 102 への会議参加時のノートパソコン PC i における処理例（その 1）を示すフローチャートである。

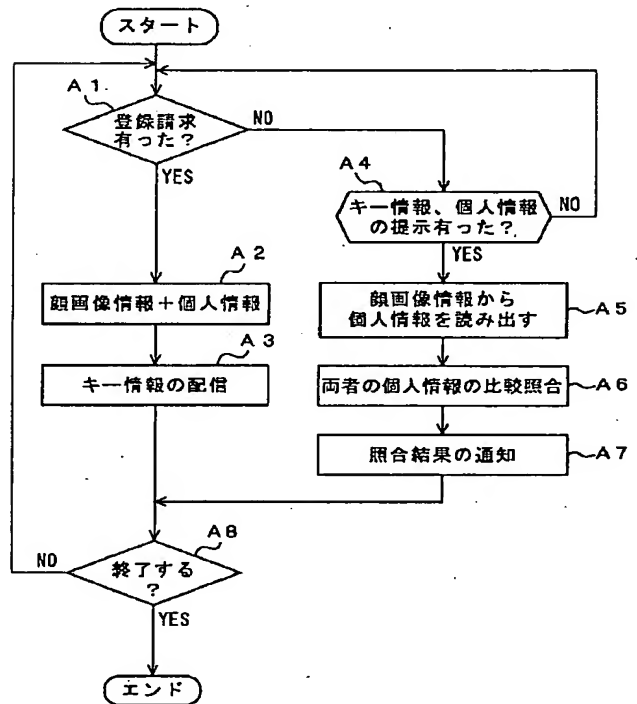
【図 15】その会議参加時のノートパソコン PC i における処理例（その 2）を示すフローチャートである。

【符号の説明】

1・・・情報処理装置、2A、2B・・・プロジェクタ、3A、3B・・・コミュニケータ、4、40・・・通信手段、8・・・マウス、10A、10B・・・プレゼンテーション装置（情報提供管理手段）、11・・・液晶ディスプレイ（表示手段）、12・・・記憶手段、13・・・制御装置、14・・・キーボード、32・・・CPU（制御装置）、34・・・データ格納装置（記憶手段）、100・・・ネットワーク情報処理システム、102・・・遠隔地間電子会議システム、PC i（i=1～n）・・・ノートパソコン（情報処理装置）

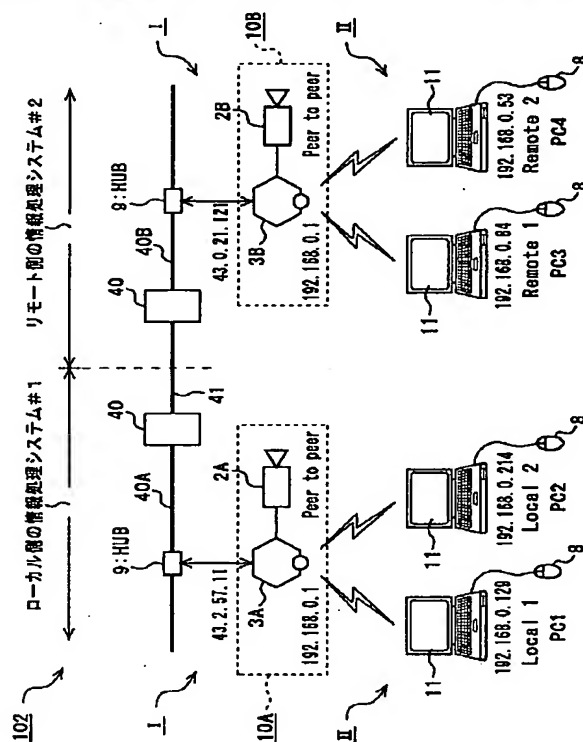
【図 2】

情報提供管理系 I における認証例



【図 4】

## 遠隔地間電子会議システム102の構成例



【图 6】

### 使用者固定データUCDのデータフォーマット例

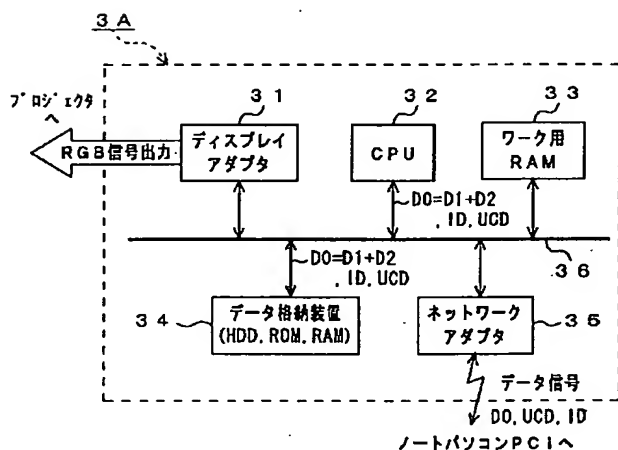
使用者固定データ (45 bytes)

ユーザー情報 (42 bytes)

UCD

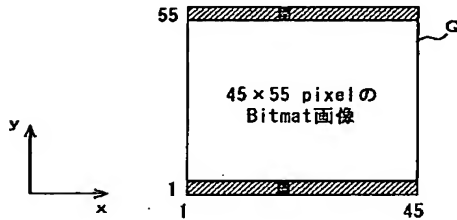
ヘッダーID (2 bytes)	ユーザー名 (12 bytes)	フルネーム (20 bytes)	ユーザーID (8 bytes)	チェックサム (RGB) (3 bytes)
---------------------	---------------------	---------------------	---------------------	---------------------------

0xEC      ライトコード [7:0]



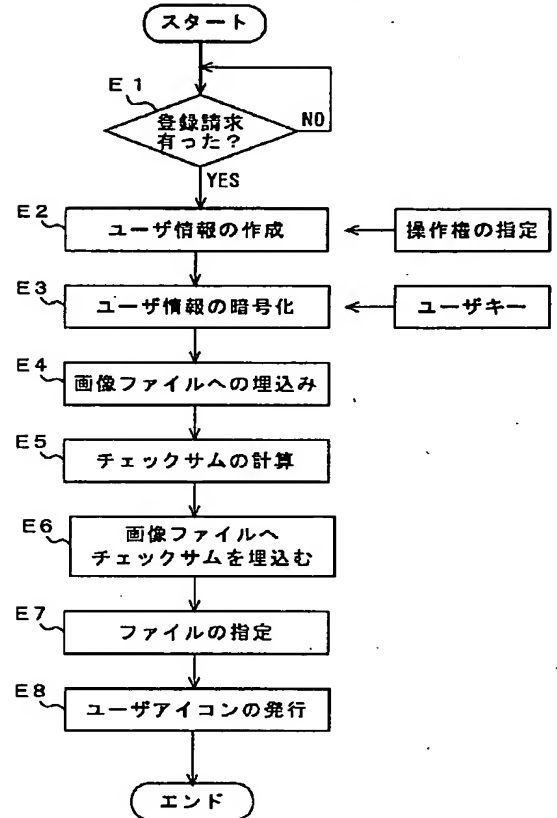
【図7】

顔画像ファイルQへの重畳(埋め込み)例



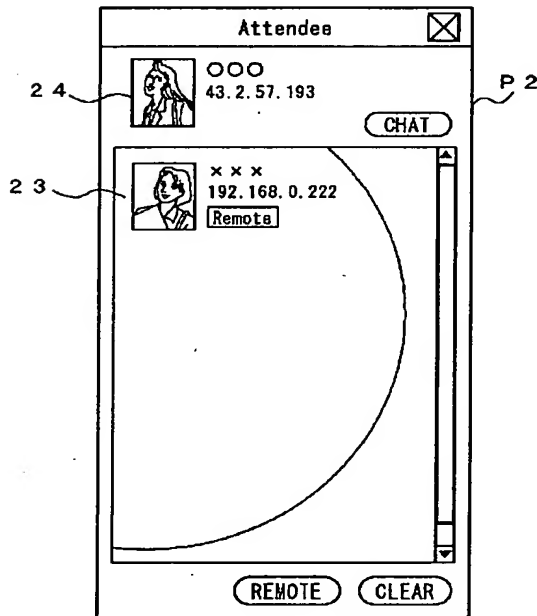
【図8】

ユーザアイコン画像の作成例



【図10】

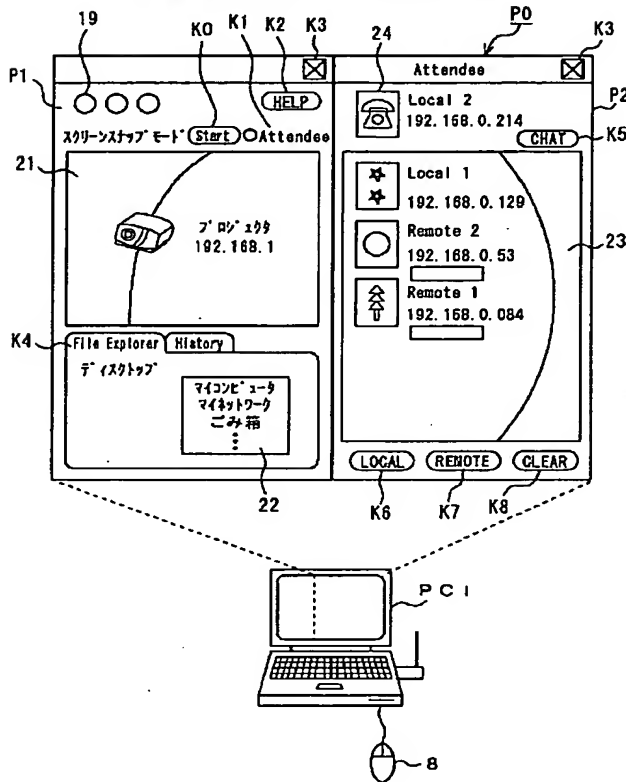
アテンディ画面P2におけるユーザアイコン画像の表示例





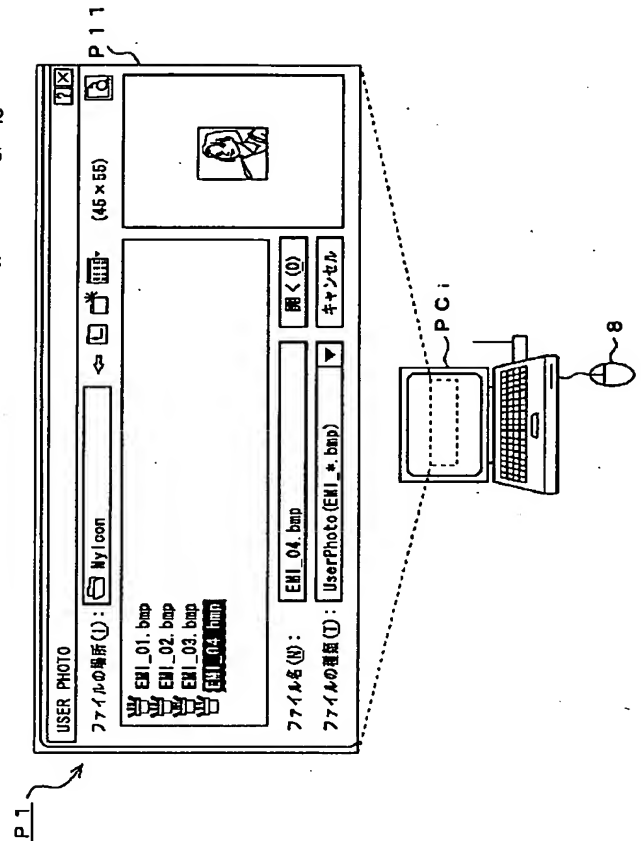
【図9】

ノートパソコンPC1におけるGUI  
起動時画面P0の表示例



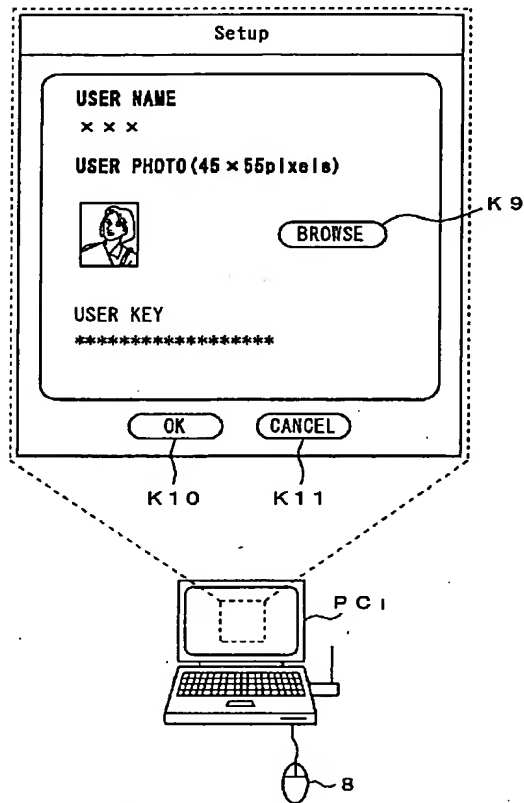
【図11】

ファイル確認画面P11の表示例



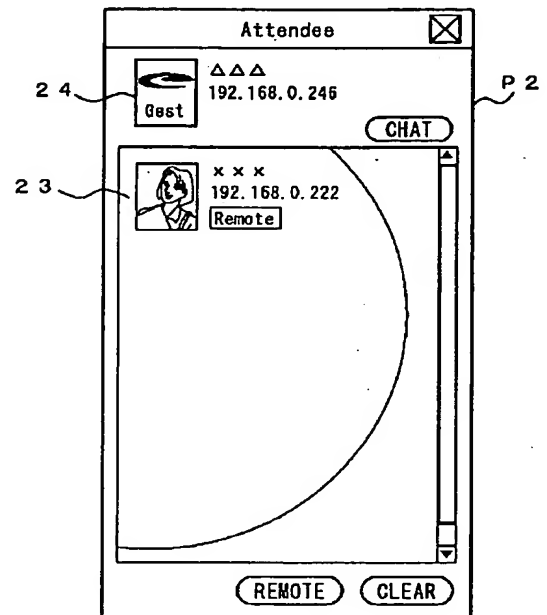
【図12】

セットアップ画面P12の表示例



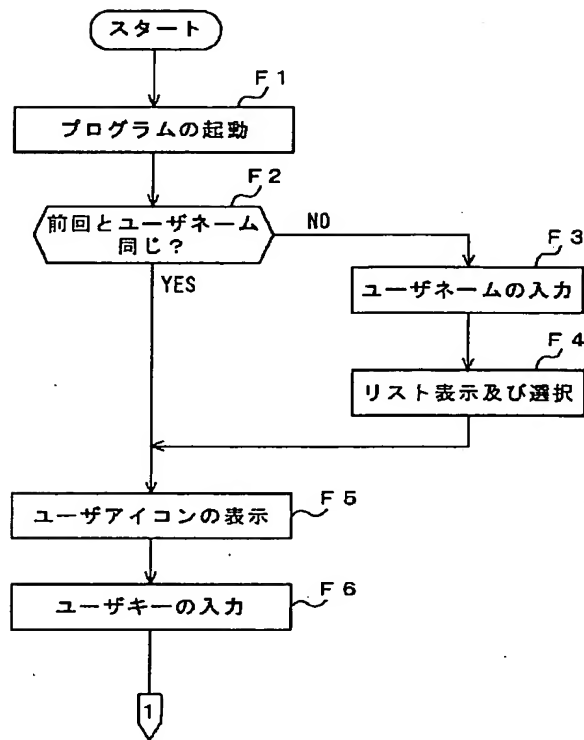
【図13】

アテンディ画面P2における制限付きユーザアイコン画像の表示例



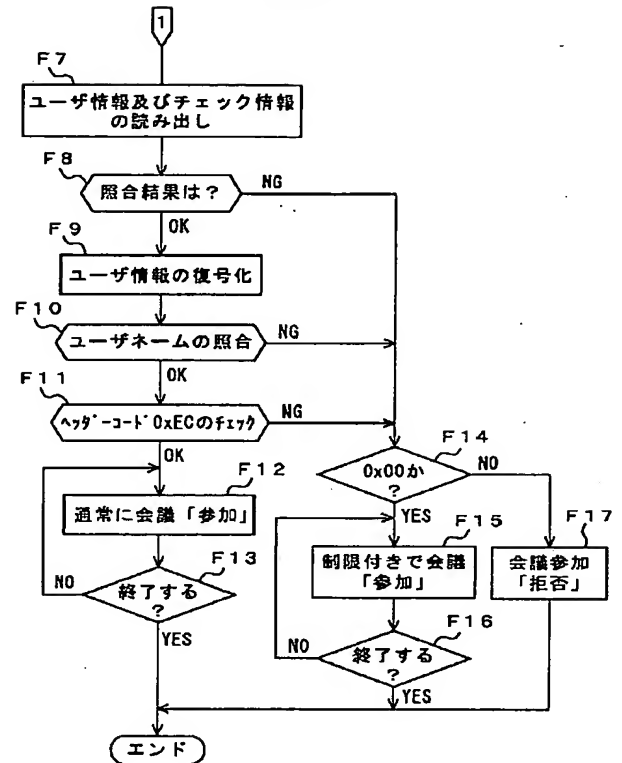
【図14】

ノートパソコンPCiにおける処理例  
(その1)



【図15】

ノートパソコンPCiにおける処理例  
(その2)



フロントページの続き

Fターム(参考) 5B057 CA01 CA08 CA12 CA16 CB01  
CB08 CB12 CB16 CC02 CE08  
5B085 AA08 AE23 AE25 BA07 BE04  
BE07 BG01 BG02 BG07  
5C064 AA02 AB03 AC08 AC22 AD06  
BB07 BC23

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☒ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☒ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**